Claims

WHAT IS CLAIMED IS:

1. A method in a computer system for identifying a principal associated with a first object comprising:

maintaining in the first object identity information identifying the principal;

invoking a method in an API with the identity information as an argument,

under control of the method,

searching a principal data store for principal data identified by the identity information;

instantiating a principal object having principal data identified by the identifying information; and

returning a pointer to the principal object or,

if more than one principal is found in the data store having the principal data, returning an error.

2. The method of claim 1 wherein the identity information is an identity reference identifying an identity claim of the principal and invoking comprises:

invoking the findbyidentity method in a principal API exposed by the principal data store with the identity reference as an argument.

3. The method of claim 1 wherein the identity information is an identity reference identifying an identity claim of the principal and invoking comprises:

invoking a findbyidentity method in a principal API exposed by the principal data store with the ItemContext as a first argument, and identity reference as a second argument; and

under control of the findbyidentity method,

searching a principal data store identified by the ItcmContext argument for a principal having the identity claim;

instantiating a principal object for the principal having the identity claim;

returning a pointer to the principal object; or,

if more than one principal is found in the data store, returning an error.

4. The method of claim 1 wherein the identity information is an identity reference identifying an identity claim of the principal, the identity reference having an identity claim value and scheme, and invoking comprises:

invoking a findbyidentity method with the identity claim value and scheme as arguments; and

under control of the findbyidentity method,

searching a principal data store for a principal having the identity claim value and scheme;

instantiating a principal object for the principal having the identity claim value and scheme;

returning a pointer to the principal object; or,

if more than one principal is found in the data store having the identity claim value and scheme, returning an error.

5. The method of claim 1 wherein the identity information is an identity reference identifying an identity claim of the principal, the identity reference having an identity claim value and scheme, and invoking comprises:

invoking a findbyidentity method with the identity claim value as an argument; and

under control of the findbyidentity method,

searching a principal data store for a principal having the identity claim value with any scheme;

instantiating a principal object for the principal having the identity claim value and scheme;

returning a pointer to the principal object; or,

if more than one principal is found in the data store having the identity claim value and scheme, returning an error.

6. The method of claim 1 wherein the identity information is an identity reference identifying an identity claim of the principal, the identity reference having an identity claim value and scheme, and invoking comprises:

invoking a findbyidentity method with the identity claim value and scheme and a principal type as arguments, the findbyidentity method in an application programming interface of the first object; and

under control of the findbyidentity method,

searching a principal data store for a principal of the principal type that also has the identity claim value and scheme;

instantiating a principal object of the principal type, the principal object having the identity claim value and scheme; and

returning a pointer to the principal object; or,

if more than one principal is found in the data store having the identity claim value and scheme, returning an error.

7. The method of claim 1 wherein the first object is an identity reference object having an identity reference and invoking comprises:

invoking a findbyidentity method with the identity reference, the findbyidentity method in an application programming interface of the first object; and

under control of the findbyidentity method,

searching a principal data store for a principal identified by the identity reference;

instantiating a principal object for the principal identified by the identity reference; and

returning a pointer to the principal object; or,

if more than one principal is found in the data store having the identity claim value and scheme, returning an error.

8. The method of claim 1 further comprising:

storing in the principal data store, principal data including at least one identity claim for every principal known to the computer system.

9. The method of claim 1, wherein the principal object includes at least one identity claim object, and the principal object and identity claim object expose application programming interfaces that have the findbyidentity method.

5

10. An application programming interface (API) for a central data store of principal objects in a computer system that is part of a distributed system, each principal object associated with one principal and having at least one property that uniquely identifies the associated principal in the distributed system, the API comprising:

a findbyidentity method that when invoked with the property searches the computer system for principal data uniquely identified by the property, instantiates a principal object containing the principal data identified by the property, and returns a pointer to the principal object.

11. The API of claim 10 wherein the API comprises:

a second findbyidentity method that when invoked with the property and an identifier identifying a data store on the computer system, searches the data store for principal data uniquely identified by the property, instantiates a principal object containing the principal data identified by the property, and returns a pointer to the principal object.

12. The API of claim 10 wherein the property comprises a value and a scheme and the API comprises:

a third findbyidentity method that when invoked with the value and an identifier identifying a data store, searches the data store for principal data uniquely identified by the value and a default scheme, instantiates a principal object containing the principal data identified by the value and the default scheme, and returns a pointer to the principal object.

13. The API of claim 10 wherein the object is an identity reference object that has a second property that is an identity reference and the API comprises:

a fourth findbyidentity method that when invoked with the identity reference and an identifier identifying a data store, searches the data store, instantiates one or more principal objects containing an identity claim matching the identity reference, and returns a pointer to the principal object.

14. A computer program product readable by a computing system and encoding a computer program of instructions for executing a computer process for identifying a principal, said computer process comprising:

maintaining in the first object identity information identifying the principal;

invoking a method in an API with the identity information as an argument,

under control of the method,

searching a principal data store for principal data identified by the identity information;

instantiating a principal object having principal data identified by the identifying information; and

returning a pointer to the principal object or,

if more than one principal is found in the data store having the principal data, returning an error.

15. The computer program product of claim 14 wherein the identity information is an identity reference identifying an identity claim of the principal and invoking comprises:

invoking the findbyidentity method in a principal API exposed by the principal data store with the identity reference as an argument.

16. The computer program product of claim 14 wherein the identity information is an identity reference identifying an identity claim of the principal and invoking comprises:

invoking a findbyidentity method in a principal API exposed by the principal data store with the identity reference as a first argument, and an ItemContext as a second argument; and

under control of the findbyidentity method,

searching a principal data store identified by the ItemContext argument for a principal having the identity claim;

instantiating a principal object for the principal having the identity claim;

returning a pointer to the principal object; or,

if more than one principal is found in the data store, returning an error.

17. The computer program product of claim 14 wherein the identity information is an identity reference identifying an identity claim of the principal, the identity reference having an identity claim value and scheme, and invoking comprises:

invoking a findbyidentity method with the identity claim value and scheme as arguments; and

under control of the findbyidentity method,

searching a principal data store for a principal having the identity claim value and scheme;

instantiating a principal object for the principal having the identity claim value and scheme;

returning a pointer to the principal object; or,

if more than one principal is found in the data store having the identity claim value and scheme, returning an error.

18. The computer program product of claim 14 further comprising:

storing in the principal data store, principal data including at least one identity claim for every principal known to the computer system.

19. The computer program product of claim 17, further comprising:

independently selecting a property from the principal data to be an identity claim, the property uniquely identifying the principal and distinguishing it from all other principals known to the computer system.

20. A method in a computer system for managing principal data, the computer system having installed thereon a plurality of disparate applications that utilize principal data, the method comprising:

storing on the computer system in a central data store principal data for a plurality of principals;

identifying for each principal, one or more identity claims that uniquely identifies the principal;

providing the plurality of disparate applications access to the principal data via component objects having at least one identity reference and capable of calling a standardized principal application programming interface (API), the standardized principal API containing methods accessing the central data store, instantiating principal objects, and retrieving principal data.

21. The method of claim 20 wherein identifying comprises:

identifying at least one identity claim for each principal known to the computer system.

22. The method of claim 21 wherein the at least one identity claim for each principal is independently selected from the group consisting of a telephone number, an email address, a name, a security identifier, a globally unique identifier, a social security number, an employee number, a student number, a drivers license number, a credit card number, and a physical address.

23. The method of claim 21 wherein the standardized principal API includes a findbyidentity method that, when passed a first identity reference, searches the central data store for the first identity claim identified by the first identity reference and instantiates a principal object having the first identity claim.

24. The method of claim 21 wherein each identity claim includes an identity claim value and an identity claim scheme and the standardized principal API includes a findbyidentity method that, when passed an identity claim value but not an identity claim scheme, searches the central data store for an identity claim of a default identity claim scheme having the identity claim value and

instantiates a principal object having an identity claim with the identity claim value and the default identity claim scheme.

25. The method of claim 21 wherein each identity claim includes an identity claim value and a identity claim scheme and the standardized principal API includes a findbyidentity method that, when passed a first identity claim value and a first identity claim scheme, searches the central data store for an identity claim having the first identity claim value and first identity claim scheme and instantiates a principal object having an identity claim with the first identity claim value and first identity claim scheme.

26. The method of claim 20 further comprising:

monitoring the data received by the plurality of disparate applications for new principal data not already stored in the central data store; and

storing the new principal data in the central data store.

27. The method of claim 21 wherein each identity claim includes an identity claim value and a identity claim scheme and the standardized principal API includes a findbyidentity method that, when passed a store identifier identifying the central store, a first identity claim value and a first identity claim scheme, searches the central data store for an identity claim having the first identity claim value and first identity claim scheme and instantiates a principal object having an identity claim with the first identity claim value and first identity claim scheme.

28. The method of claim 21 wherein each identity claim includes an identity claim value and a identity claim scheme and the standardized principal API includes a findbyidentity method that, when passed a principal type identifier identifying a first principal type, a first identity claim value and a first identity claim scheme, searches the central data store for a principal of the first principal type having an identity claim having the first identity claim value and first identity claim scheme and instantiates a principal object having an identity claim with the first identity claim value and first identity claim scheme.

29. The method of claim 21 wherein each principal includes one or more identity claims and the standardized principal API includes a findbyidentity method that, when passed a first identity reference, searches the central data store for principals having the first identity claim identified by the identity reference and instantiates the principal object having an the first identity reference.

30. The method of claim 29 wherein each identity reference includes an identity reference value and a identity reference scheme and the standardized principal API includes a findbyidentity method that, when passed a first identity reference value but not an identity reference scheme, searches the central data store and instantiates a principal object having an identity claim having the first identity reference value and a default identity reference scheme.

31. A method in a computer system for determining a first identity reference of a first type of a principal from a second identity reference property of the principal comprising:

using the second identity reference to identify a principal;

instantiating a principal object for the principal, the principal object having a first identity claim of the first type identified by the first identity reference and a second identity claim of a different type identified by the second identity reference;

invoking a translate function exposed by the principal object with the first type as an argument;

receiving the first identity reference.

32. The method of claim 31, wherein the principal object includes a first identity claim object having the first identity claim and a second identity claim object having the second identity claim and invoking comprises:

invoking the translate function in the second identity claim object.

33. The method of claim 32 further comprising:

under control of the translate function,

searching the identity claim objects of the principal object for an identity claim object with an identity claim of the first type; and

returning a pointer to the first identity claim object.

34. The method of claim 31, wherein using comprises:

invoking a findbyidentity method of a principal API with the second identity reference as an argument.

35. The method of claim 32, wherein using further comprises:

receiving a pointer to the second identity claim object of the principal object.